bind()

Race and conflict conditions with mulitple processes or threads attempting to bind to the same port and IP adress

Sean Barnum, Cigital, Inc. [vita[1]]

2005-10-03

Onderdeel "Original Cigital Coding Rule in XML"

Mime-type: text/xml, omvang: 3468 bytes

Identification Difficulty

Scan

Rule Accuracy

False Negatives

Priority

Low

Attack Categories

- Denial of Service

Vulnerability Categories

- Race Condition

Software Context

Networking

Description

bind() takes an unnamed socket and assigns a name to it. This name, in the case of a network socket, is an IP address and a port. If two processes (or even two threads) want to bind to the same port at the same IP address, a race condition will exist and only one process will be allowed to have the port. The other call will return an error. Also, if a server binds to a socket interface with a ‘vague’ address first (say, all

1. daisy:35 (Barnum, Sean)

IP addresses) and then another server binds with more specific address (say, 192.158.2.27, the IP of the box) then the second server will get the traffic. A Windows addition has been made to remedy this setsockopt(...SO_EXCLUSIVEADDRUSE,...)

Application Programming Interfaces

Function Name	Comments
bind()	

Method of Attack

An attacker could write another program to open the same port on the same IP address that he or she knows the target program will. When the target program tries to do so, it will fail and access to the service it provides will be denied. Bind can also be used maliciously

Solutions

Applicability	Description	Efficacy
This solution is applicable if the host is a running a Unix-based operating system and the process is being run with super-user privileges.	Bind to a port lower than 1024. Only processes run by the super-user have the ability to bind to these ports.	Binding to a port lower than 1024 will restrict which processes can compete for access to the same port on the same IP.

Signature Details

```
int bind(int s, const struct sockaddr *name, socklen_t namelen);
```

Source References

- ITS4 Source Code Vulnerability Scanning Tool - http://www.cigital.com/its4/
- bind() man page: http://www.hmug.org/man/2/bind.php
- Howard, Michael & LeBlanc, David C. Writing Secure Code, 2nd ed. Redmond, WA: Microsoft Press, 2002, ISBN: 0735617228.

Discriminant Set

Operating Systems

- UNIX (All)

Languages

- C

- C++

Cigital, Inc. Copyright

Velden

Naam	Waarde
Copyright Holder	Cigital, Inc.

Velden

Naam	Waarde
Attack Categories	Denial of Service
Operating System	UNIX (all)
Software Context	Networking
Vulnerability Categories	Race Condition

1. mailto:copyright@cigital.com